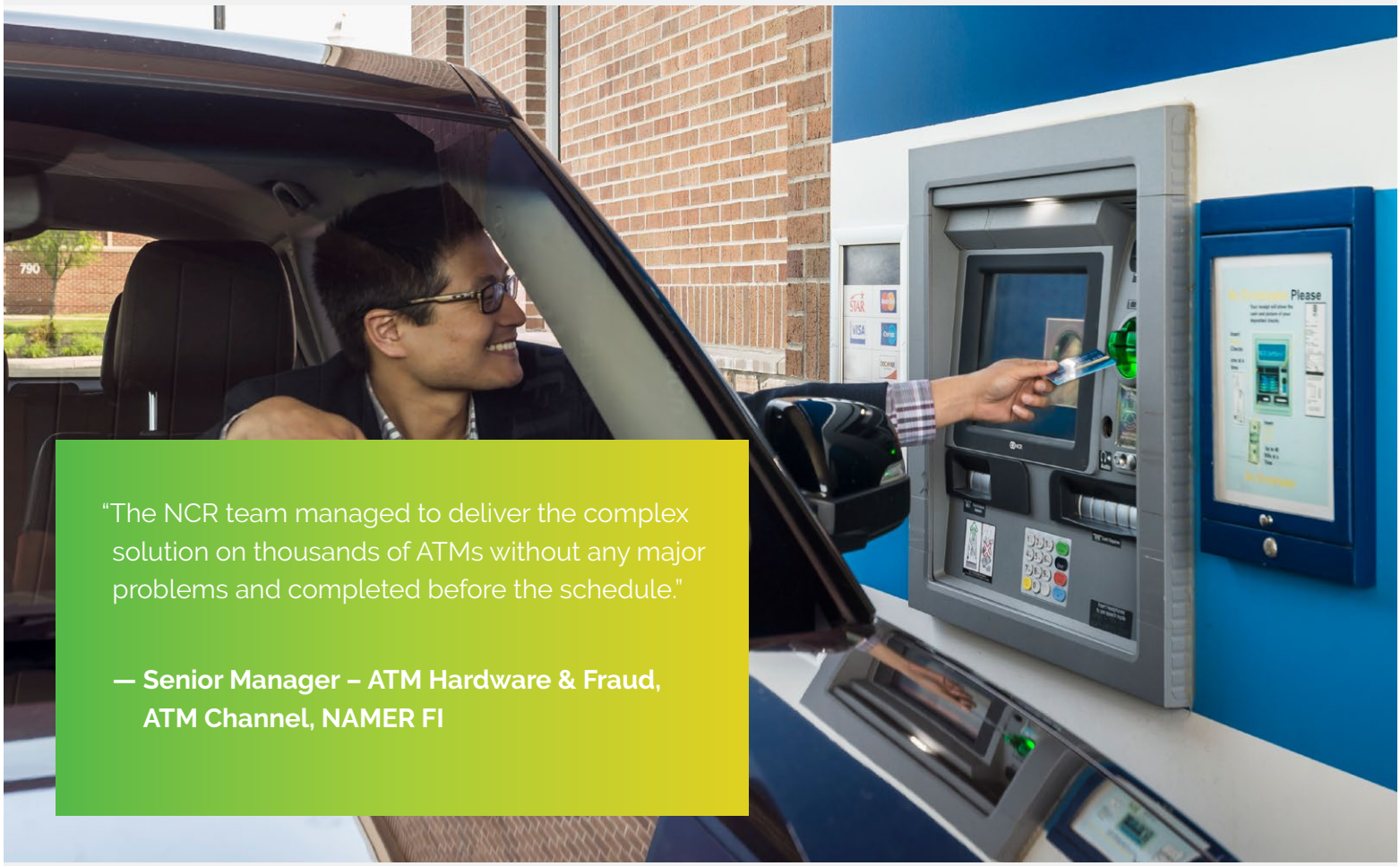
NCR SKIMMING PROTECTION SOLUTION ELIMINATES CARD SKIMMING LOSSES

The bank saw complete elimination of card skimming attacks and significant decrease in false alerts.



"The NCR team managed to deliver the complex solution on thousands of ATMs without any major problems and completed before the schedule."

— Senior Manager – ATM Hardware & Fraud, ATM Channel, NAMER FI

For more information, visit ncr.com, or email ncr.financial@ncr.com.

KEY HIGHLIGHTS

Industry/Market:
Retail Banking

Challenge:
The customer was experiencing high levels of false alerts from older versions of anti-skimming solutions. These alerts created additional workloads on the banks Fraud group to investigate if the attacks were legitimate.

Solution:
NCR Skimming Protection Solution disrupts the operation of the ATM when there is any attempt by a criminal to record data via their skimming device from the magnetic stripe on the card.

Results:
- The customer worked with NCR to deploy all of their ATMs with NCR Skimming Protection Solution (over 3,000 ATMs)
- The deployment was completed ahead of schedule

THE CUSTOMER

This customer is a North America based national bank.

THE CHALLENGE

Between 2012 and 2014 the bank was experiencing one or two ATM card skimming attacks a month. The losses were consistent with the industry average of $40,000 – $50,000 per skimming incident. Not to mention the corresponding negative impact to the bank's brand and customer service levels.

ATM Skimming continues to become more sophisticated with the entry of organized crime. Skimming devices are getting smaller and undetectable. With the help of mobile phone technology, criminals are creating ATM PIN capture devices that can also send the image to a remote PC.

There are certain trends related to ATM skimming attacks:

- The crime constantly evolves
- The criminals become ever more organized
- The crime ever more sophisticated
- Criminals migrate to the weakest link
- Skimming devices get smaller and harder to defeat

As a result, there remains a constant and global increase in card fraud which results in the following:

- Consumers trust in the Financial Institution is damaged
- Recognition that reputation and integrity of brand and customer loyalty is priceless
- Hard cash losses associated with crime

THE SOLUTION

The customer chose NCR Skimming Protection Solution to address their continuing situation with ATM skimming attacks. NCR Skimming Protection Solution is designed specifically for NCR ATMs and provides comprehensive protections through functionality to detect and jam most forms of bezel and insert skimmers. It provides additional anti-tampering sensors to protect the device from being disabled with sabotage and also provides physical protection components to prevent other forms of skimming attacks.

Detection and disruption technology

Detection is focused on the card data path, which minimizes the potential for false alerts. Integration with the ATM triggers both physical barriers to prevent cards from being inserted into the ATM. Customers can have the option to take the ATM out of service until the detected object is removed. (Note the customer in this case study did not choose this implementation option.)

Multiple sensors create a constantly changing random stream of noise to disrupt and jam any devices that may attempt to take a clean read of cardholder data. The customer was particularly impressed with the way the NCR solution deployed Jamming technology. The customer viewed this as a key differentiator for the solution. This means when a criminal takes their skimmer or recording device away, they cannot decipher the cardholder's data.

Integrated diagnostics and state of health

Unlike third party solutions, SPS has built in diagnostics and state of health so that the deployers can monitor the device and pinpoint whether it is functional or not; if it is not — action can be taken.

Future-ready solution architecture

SPS uses industry standard expandable bus architecture & new sensors and alarm devices can be added in the future to protect from new types of attack without having to replace the SPS module — fast response to new threats.

SPS uses Field Programmable Gateway Array (FPGA) architecture — so hardware can be repurposed via downloadable software.

Remote monitoring and superior manageability

Different software implementation scenarios are possible, depending on the target network environment. SPS will send status messages to XFS via the SUI Service Provider, and through SNMP. NCR Skimming Protection Solution can also operate in a standalone mode as well.

THE SOLUTION BENEFITS

The benefits of NCR Skimming Protection Solution were immediately apparent. Upon deployment the bank saw the complete elimination of card skimming attacks in the ATM channel. All 4,600 of the bank's ATMs are now under the protection of NCR Skimming Protection Solution. The deployment was completed ahead of schedule.

THE CUSTOMER VIEW

"The NCR team managed to deliver the complex solution on thousands of ATMs without any major problems and completed before the schedule."

"Execution of the plan was top notch with no effect on the bank clients, without a single complaint to the bank."

"The bank is extremely satisfied with the solution and the service provided by NCR."

— Senior Manager – ATM Hardware & Fraud, ATM Channel, NAMER FI

WHY NCR?

NCR Corporation (NYSE: NCR) is a leader in omni-channel solutions, turning everyday interactions with businesses into exceptional experiences. With its software, hardware, and portfolio of services, NCR enables nearly 700 million transactions daily across retail, financial, travel, hospitality, telecom and technology, and small business. NCR solutions run the everyday transactions that make your life easier.

NCR is headquartered in Atlanta, Ga., with over 30,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries.